

Security Engineering: Systems Engineering of Security through the Adaptation and Application of Risk Management

David P. Gilliam and Martin S. Feather
Jet Propulsion Laboratory, California Institute of Technology
4800 Oak Grove Dr.
Pasadena, CA 91109
david.p.gilliam@jpl.nasa.gov, martin.s.feather@jpl.nasa.gov

Abstract. Information Technology (IT) Security Risk Management is a critical task in the organization, which must protect its resources and data against the loss of confidentiality, integrity, and availability. As systems become more complex and diverse, and more vulnerabilities are discovered while attacks from intrusions and malicious content increase, it is becoming increasingly difficult to manage IT security. This paper describes an approach to address IT security risk through risk management and mitigation in both the institution and in the project life cycle. The application of risk management to security engineering is described. Support for this through application of a security risk algorithm and a risk management tool for risk analysis is also discussed.

Introduction

Engineering Information Technology (IT) security is a critical task to manage in the organization. With the growing number of system security defects being discovered and as the impact of malicious code continues to grow, Systems Engineering (SE) of IT security is a critical task both organizationally and in the project life cycle. Organizations have suffered significantly over the last few years due to the loss of Confidentiality, Integrity, and Availability (CIA) of IT resources due to malicious code attacks and break-ins. Understanding and mitigating these risks is paramount in protecting organizational resources. The problem has been noted by the United States (US) Government Accounting Office (GAO), showing that US federal agencies are at high risk. In a recent audit of the US Department of Defense (DoD), the GAO reported, "Security assessments continue to identify weaknesses that could seriously jeopardize DoD's operations and compromise the confidentiality, integrity, or availability (CIA) of sensitive information ... Specifically, the Inspector General found security lapses relating to access to data, risk assessments, sensitive data identification, access controls, password management, audit logs, application development and change controls, segregation of duties, service continuity, and system software controls, among others." (GAO-03-98 2003)

This paper will explore the need for Security Engineering in the System Development Life Cycle (SDLC), the role of the Security Engineer, security risk management, including security risk identification, impact, and mitigations. A process for security risk management is described along with a process to integrate it into the life cycle. Risk-Informed systems engineering is discussed, with a description of how a JPL-developed risk management tool could be used to support this. Finally, the discussion will focus on a roadmap for institutional and project security engineering.

MANAGING COMPLEXITY AND CHANGE!
INCOSE 2004 - 14th Annual International Symposium Proceedings

IT Security and the need for Security Engineering. Engineering IT Security is a specialized area of concern both for organizations and projects. If security is not a part of the life cycle in product development, the quality of the product could be impacted, and the result could be loss of trust and public image. On-line banking or purchasing systems require that security be an end-to-end process throughout the product life cycle. As systems become more complex and extensive organizationally, engineering security in the IT environment is increasingly difficult. Controls to identify and manage security risks are available. However, they are applied non-uniformly, leaving the organization vulnerable to the “weakest link” factor. A uniform approach that integrates both institutional and project risk analysis and mitigations is needed. A formal System Security Engineering (SSE) approach that identifies security risk, mitigations, and ensures that security requirements are instantiated in the organization and Systems Development Life Cycle (SDLC) will aid in identifying risks and mitigations (Stoneburner et al 2001).

Security Engineering - Systems Engineering (SE) of IT System Security. Security Engineering is not a topic that is normally addressed in courses and books on systems engineering. Yet, security engineering is a critical task (Anderson 2001). The number of US agencies devoted to security, including the new US Department of Homeland Security, shows that security is now taken very seriously as a SE discipline. Security is a complex task that requires collaboration between management, IT security professionals, system engineers, and other stakeholders. It begins early in the SDLC (knowing and understanding customer needs, government regulations, stakeholder requirements, etc.). The goal is to identify security risks and provide a means to manage, mitigate, and/or accept the risks and then ensure that SSE is sustained throughout the SDLC (McGraw 1999). Systems Engineering is needed in multiple environments, on multiple scales, from large systems like nuclear power plants, major defense systems, to smaller systems that protect intellectual property—keys to corporate assets. It encompasses or touches on several domain areas including physical security, continuity of operations (disaster preparedness), identity protection, and data security. In each of these domains security must protect CIA. It requires a specialized knowledge and skill set. An SSE must be knowledgeable of applicable organizational, government, and other governing security regulations, policies, standards, guidelines (and best practices). An SSE must also be knowledgeable of formal tools and their uses in the SDLC.

Application of Risk Management to System Security Engineering (SSE). When Risk and Risk Management are used in reference to security the discussions generally focus on defining and describing IT security risk in terms of protection of data and system Confidentiality, Integrity and Availability (CIA). These terms are commonly defined as:

- *Confidentiality:* Assuring information will be kept secret, with access limited to appropriate persons. For Intellectual property or medical information, confidentiality is a critical issue.
- *Integrity:* Assuring information will not be accidentally or maliciously altered or destroyed. Loss of Integrity is a critical issue for data on which decisions are based.
- *Availability:* Assuring information and communication services will be ready for use when expected. An attack can impact a critical system that is dependent on high availability.

Risk Management has been defined as “a proactive, continuous and iterative process to manage risk to achieve the planned objectives. The process involves identifying, analyzing, planning, tracking, controlling, documenting, and communicating risks effectively” (see Figure 1). (NASA CRM). In application to security, risk is a function of the *impact* an adverse event

MANAGING COMPLEXITY AND CHANGE!
INCOSE 2004 - 14th Annual International Symposium Proceedings

would have were it to succeed in breaching defenses, its *likelihood of succeeding*, and the *frequency* at which such events are perpetrated. Quantifying risk in these terms depends on the relative value of the potential loss or disruption should the risk event occur. A formula to quantify IT security risk is defined here as: $Risk = impact * likelihood * frequency$ — Where:

$Impact = damage * recovery\ time$

- Damage can be characterized as the criticality of the data and IT resources along with the degree and extent of their destruction or loss – that is, the criticality of the data and resources and the degree and extent of the loss or compromise. Degree is the damage to a system or set of resources, with extent being the number of systems affected and/or amount of data compromised. A key approach to decreasing risk is to adopt measures that reduce the damage should security attacks succeed in breaching defenses.
- Recovery time is the length of time to recover data and IT resources from a compromise, or the time needed to return to operations should recovery be unfeasible or unneeded.

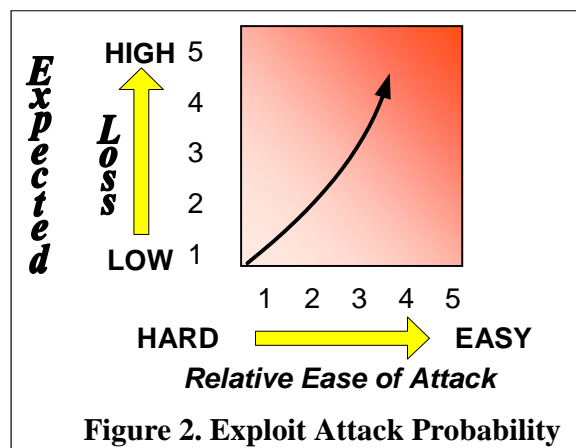
$Likelihood = potential\ success\ of\ an\ attack$

- Likelihood is the potential that the attack succeeds, and therefore leads to loss or compromise of CIA. A key approach to decreasing risk is to adopt defenses that make attacks less likely to succeed (e.g., training users on selection of passwords so that it is less likely that password hacking will succeed in locating a valid password or applying security patches).

$Frequency = number / time, where\ number = ease * likelihood * impact$

- Number is the number of events occurring over a time interval
- The frequency of an exploit being perpetrated is based on three factors: how easy it is to originate an attack, how likely that attack is to succeed, and how much impact it will have if it does succeed – this combination reflects the malicious intent of would-be attackers.

A consequence of this equation is that the factors of *likelihood* and *impact* occur twice in the overall formula: $Risk = impact * likelihood * frequency = impact * likelihood * (ease * likelihood * impact) = impact^2 * likelihood^2 * ease$. The key characteristic of SE (compared to safety engineering) is the malicious intent of the attackers, who deliberately favor attacks that they perceive have a greater potential for success and a greater propensity for damage.



MANAGING COMPLEXITY AND CHANGE!

INCOSE 2004 - 14th Annual International Symposium Proceedings

Attack sophistication and complexity are unpredictable and these must factor into risks and their mitigations. Damage is premised on the fact that attacks that are easier to carry out and that result in greater harm will occur more often (Figure 2). However, it is difficult to predict new attacks and attack types. System complexity factors and sophistication of attacks create events that must be evaluated as they occur. For this reason IT security risk management must be a persistent process. The threat scenario is continually changing and risk management must be able to respond to the changing environment as well as take advantage of better mitigations.

SSE includes identification of: 1) controlling policies, standards, guidelines, and best practices, 2) the relative likelihood of the risk being realized, and 3) the potential impact of accepting risk. Decomposing the governing policies, standards, and requirements from the customer and stakeholders into their basic constituent elements is needed to properly assess the acceptable levels of risk and extent and cost to mitigate them. Use of a risk assessment tool is highly beneficial and recommended to facilitate this process (Gilb 2003, RiskWatch 2003). The risk assessment should identify the relative cost of the risk in terms of the potential impact to the organization, and the relative cost to mitigate those risks. The process involves groups of domain experts who identify risks and their mitigations. The whole process is controlled by a System Security Engineer (SSE), who works with these groups and with management to control risks. Figure 3 shows a process that is controlled by the SSE to identify and manage these risks.

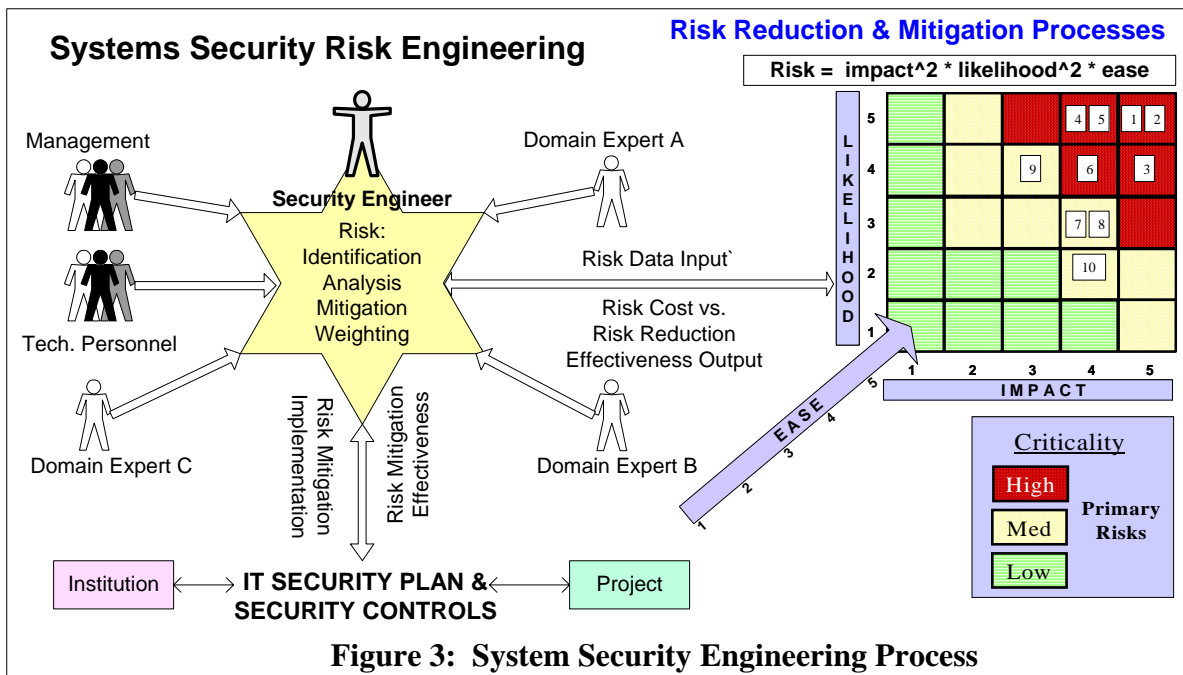


Figure 3: System Security Engineering Process

Related Work. The Gartner Group in identifying the cornerstones of an InfoSec (Information Security) risk management program makes the point that “IT assets that put an enterprise at risk must be identified through an IT risk assessment inventory that covers multiple domains in an organization.” (Witty 2002). Not directly included in their assessment is IT SSE in the SDLC. Other security risk management approaches also address enterprise security risk management from a system or site qualification perspective (McGraw 1999, RiskWatch 2003, ArcSight 2003). Carnegie Mellon’s Software Engineering Institute provides several publications and a

MANAGING COMPLEXITY AND CHANGE! INCOSE 2004 - 14th Annual International Symposium Proceedings

method for security risk management called “Octave” (SEI 2003). The method provides detailed processes, worksheets and guides for a team to conduct a risk evaluation for their organization.

Security engineering is now just beginning to be addressed in the SDLC, as depicted by the recent number of books, articles, and other publications that are now being published on the subject, e.g., (Bishop 2002, Anderson 2001, Howard et al 2002). These works present a system life cycle approach that addresses requirements, design, development, operations and maintenance. However, these approaches generally do not cover the relationship and integration of the SDLC and institutional risk management processes. Additionally, often the process of phasing out software and systems is not fully addressed. When they are phased out, security exposures and vulnerabilities may be present, especially if other systems are dependent on receiving data from them and the people responsible for these systems have not been notified. There may be processes that are dependent on the phased out systems and removing software or systems without consideration of these dependencies may inadvertently expose systems to security risk through open ports or other processes on a system that is now exposed.

Risk-informed Systems Engineering

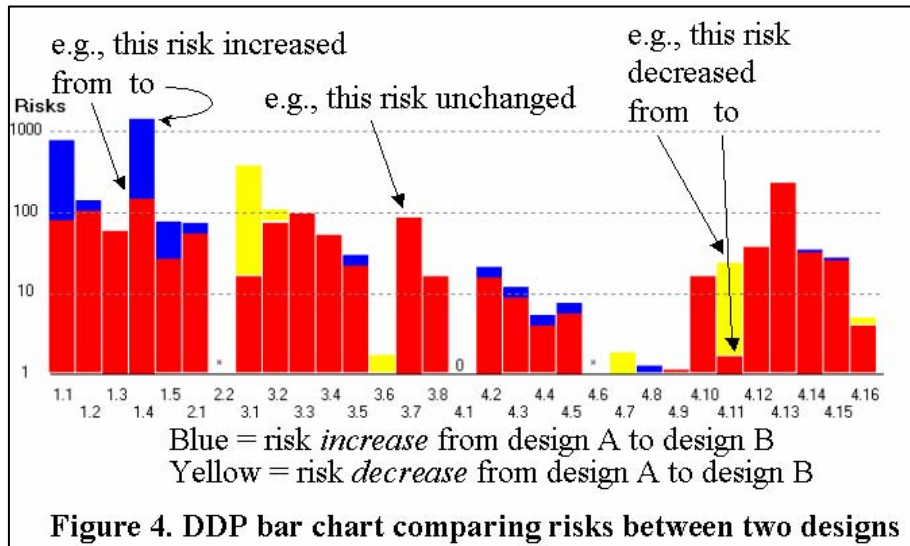
IT Security Risk and the SDLC. What still needs addressing is engineering IT security in the project life cycle so as to identify security requirements and controls for the SDLC, and integrate them with institutional risk management practices. SSE requires a team approach to assess, plan and conduct effective management of security risks. We describe the basis for such an approach next.

Defect Detection and Prevention (DDP), a Process & Tool for Risk-informed Systems Engineering. Within JPL and NASA we have been involved in the development and application of a process for risk-informed decision-making. Our process, called “Defect Detection and Prevention (DDP)”, has the goal to “facilitate risk management over the entire project life cycle beginning with architectural and advanced technology decisions all the way through operation.” (Cornford et al 2003). DDP’s origin is a structured method for planning the quality assurance of hardware systems. Since then its scope has expanded to also encompass decision-making earlier in the development lifecycle, and to be applicable to software, hardware and systems (Feather et al, 2003). Its closest mainstream equivalent is Quality Function Deployment (QFD) (Akao 1999). The DDP model is specialized to risk concerns, and adopts a probabilistic interpretation of risk that is suited to the quantitative evaluations necessary in order to employ automated search. More details of DDP, and the tool support we have built to support it, can be found at <http://ddptool.jpl.nasa.gov>

Support for decision-making *early* in the project life cycle risk management and mitigation is now the leading application area of DDP. Used at this stage, it provides support for making risk-based cost and functionality tradeoff. DDP assists project stakeholders in identifying the relative risks associated with a system, the relative cost of mitigating the risks and the trade-offs in risk mitigation and acceptance. As described in (Cornford et al 2003), “DDP explicitly represents risks, the objectives that risks threaten, and the mitigations available for risk reduction. By linking these three concepts, DDP is able to represent and reason about the cost-effectiveness of risk reduction alternatives.” The DDP process brings together stakeholders in the project who are domain experts and who represent the life cycle phases from inception to termination. This multi-disciplinary approach to risk management in the project life cycle is key to the strength of DDP. Custom software supports the DDP process, pooling the combined inputs of the domain

MANAGING COMPLEXITY AND CHANGE!
INCOSE 2004 - 14th Annual International Symposium Proceedings

experts and performing calculations over the entire body of gathered information providing aggregate risk calculation information and searches for near-optimal solutions for mitigating risks. It provides coherent visualizations of the data back to these domain experts allowing them to make well-informed decisions on risk mitigations and risk acceptance (Feather & Cornford, 2003).



DDP Risk Analysis: when using DDP, inputs to the risk analysis process estimates of risks, mitigations to the risks, and associated weightings for risk and risk mitigations. The results of a DDP risk assessment/mitigation analysis are output through a variety of graphical presentations. Figure 4 shows an example of a bar chart display of risks used to show the magnitude of risks, and how they change, between two different design solutions. The DDP tool allows for a number of various types of output sorting: by residual risk, weighting, total risk, etc. It provides drill-down capabilities to view the different risk factors and the mitigations that can be applied. Overall, these visualization capabilities have proven helpful for gaining understanding of risks and the combined effectiveness of options available for reducing risks.

Adaptation and Application of DDP to Security Engineering. Our aim is to adapt and apply DDP to the challenges of Security Engineering. As illustration, we present a preliminary example using DDP in this arena. We stress that this is preliminary – it will take significant additional work to extend this to the breadth and depth that a realistic study of security concerns warrants.

The heart of the example lies in the lists of risks and mitigations (options for reducing those risks). These are shown below.

Risks

- 1: simple password hacking
- 2: sophisticated password hacking
- 3: Open ports availability
- 4: malicious website code allows download of SAM DB
- 5: malicious code that passes information off to another location
- 6: Buffer overflows
- 7: Non-compliant users

MANAGING COMPLEXITY AND CHANGE!
INCOSE 2004 - 14th Annual International Symposium Proceedings

Mitigations

- 1: Use of VPN
- 2: Institutional firewall
- 3: SysAdmins keep patches up to date
- 4: Train users on selection of passwords
- 5: Use an IDS system and respond to its alerts
- 6: Keep critical data encrypted
- 7: Host-based firewalls
- 8: Security scans
- 9: Patches

Figure 5 shows the DDP matrix that connects these two lists – columns in the matrix corresponds to risks (named in the top row), and rows to mitigations (named in the left column); the inner (white background) cells indicate how effectively the corresponding mitigation, if applied, serves to reduce the corresponding risk. Effectiveness is indicated by a number in the range 0 – 1 (a blank cell is equivalent to 0), where the numerical value indicates the proportion of risk reduction. Highlighted in red is the column corresponding to the risk of “simple password hacking”, and highlighted in green the row corresponding to the mitigation of “Train users on selection of passwords”. The cell at their intersection holds the value “0.9”, indicating that the mitigation, if applied, will reduce the risk by a proportion of 0.9 (i.e., 90%). The kinds of numbers seen in this matrix are typical of DDP when applied for overall decision-making – it is only possible to make relatively crude estimates of effectiveness. Nevertheless, the accumulation of these is sufficient to lead to interesting insights and guidance to decision making.

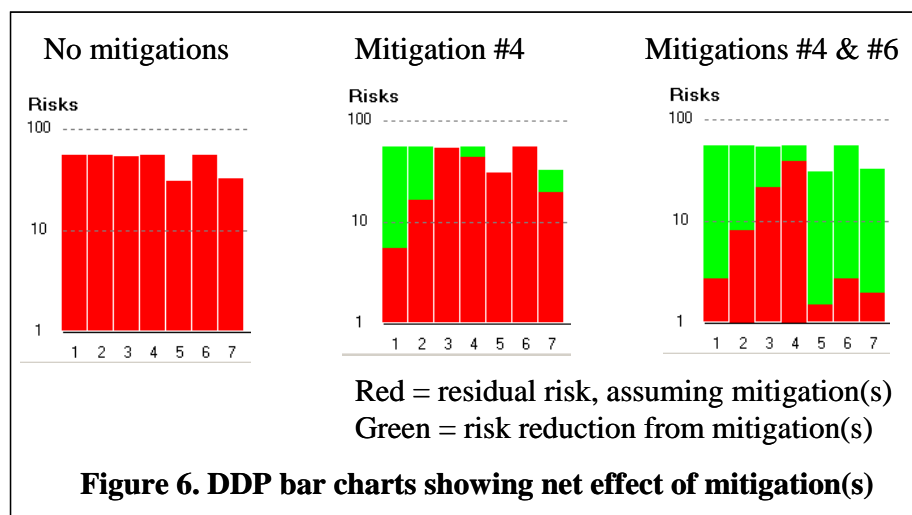
Mitgn x Risk Col = simple password hacking Row = Train users on selection of passwords								
	Risks	simple password hacking	sophisticated password hacking	Open ports availability	malicious website code allows download of SAM DB	malicious code that passes information off to another location	Buffer overflows	Non-compliant users
Mitgns	counts	8	7	7	7	5	7	9
Use of VPN	3	0.8	0.8					0.8
Institutional firewall	7	0.5	0.5	0.6	0.5	0.1	0.3	0.1
SysAdmins keep patches up to date	6	0.1	0.1	0.9	0.8		0.95	0.5
Train users on selection of passwords	4	0.9	0.7		0.2			0.4
Use an IDS system and respond to its alerts	7	0.2	0.2	0.4	0.9	0.8	0.75	0.4
Keep critical data encrypted	7	0.5	0.5	0.6	0.1	0.95	0.95	0.9
Host-based firewalls	7	0.95	0.95	0.7	0.2	0.1	0.5	0.5
Security scans	4	0.95		0.95			0.95	0.7
Patches	5			0.5	0.95	0.8	0.99	0.1

Figure 5. DDP matrix relating Mitigations (rows) to Risks (columns)

MANAGING COMPLEXITY AND CHANGE! INCOSE 2004 - 14th Annual International Symposium Proceedings

Each mitigation is an option – we can choose to do it, or not do it. If a mitigation is chosen, its risk reducing effect will be taken into account in DDP’s calculations of risk. Figure 6 shows three instances of DDP’s bar chart display of risk magnitudes. The leftmost chart shows the totally unmitigated risk magnitudes (in our preliminary example we make some minor distinction between these risks; in a realistic study, there would be more risks, and more variety among them). The center chart shows the effect of applying the mitigation #4, which was “Train users on selection of passwords”; red indicates the residual risk, assuming that mitigation, and green indicates the original level from which risk has been reduced. The display of the green is optional – presumably what decision makers ultimately care about is the residual risk. However, the green serves to indicate the risk reduction that the current set of mitigations conveys (as was seen in the earlier Figure 4, it is possible to use DDP bar charts to display risk differences between different selections of mitigations). The chart to the right shows the net effect of two mitigations, #4 (“Train users on selection of passwords”) and #6 (“Keep critical data encrypted”). Residual levels of risks are correspondingly lower, but some risks remain high, notably risk #4 (“malicious website code allows download of SAM DB”), because neither of the selected mitigations are particularly effective at reducing that risk – the matrix values (as shown in Figure 4) are 0.2 and 0.1 respectively. DDP’s rule for calculating their combination is to treat them as filtering out their respective proportion of risks, so if the first filters out 0.2 of the risk, that leaves 0.8 of the risk for the second, which in turn filters out 0.1 of that, leaving 0.72 of the risk overall. Note that DDP charts use *log* scales to plot risk magnitudes, since in most of our applications the desire is to reduce risk to quite low levels, for which log scale plots are well suited to the display of risk.

The above has concentrated on the calculation and display of the *effectiveness* (in terms of risk reduction) of a selection of mitigations. DDP also calculates the *cost* of mitigation selections. For example, the rightmost bar chart of Figure 6 portrays the case of two mitigations, so the total cost will be the sum of their individual costs. When the cost of all mitigations exceeds the resources available, there is the need to judiciously select mitigations that in concert cost-effectively reduce risk. Given the budget and schedule pressures prevalent in most situations, there is almost always the need to do this.



MANAGING COMPLEXITY AND CHANGE! INCOSE 2004 - 14th Annual International Symposium Proceedings

To extend this example to a realistic study of risk mitigation in the security realm will require further work to:

- populate the DDP tool with security information (additional risks and mitigations, mitigation costs, and the effectiveness values that connect them, as well as more information on the objectives from which the risks derive their magnitudes)
- change DDP's internal calculation of risk to the formula described earlier, $Risk = impact * likelihood * frequency$ where *frequency* is proportional to *impact*, etc. Currently DDP is set to calculate risk as simply $impact * likelihood$. The hallmark of security engineering (as compared to safety engineering) is the malicious intent of the attackers, who deliberately favor attacks that they perceive have a greater likelihood of success and a greater propensity for damage should they succeed. By this change to DDP's internal risk calculation formula this aspect of security engineering can be accommodated.

A Roadmap for Institutional and Project Security Engineering

Risk-informed Institutional Security Engineering. The value exemplified by the DDP approach is that it brings domain experts together to manage risk. Such an approach needs to be continued throughout the lifecycle. The IT environment changes over time, which affects risks and mitigations. The phases for coding, testing, validation, operations and maintenance must be a persistent process. Some of the critical areas are requirements gathering, specification and design to measurable requirements (Gilb 2003). Implementation and operations also need addressing, such as updated operations manuals, removal of installation files which can be used to overwrite current configuration settings, or configuration settings left in an unsecured state after installation (usually settings are left at the default which generally has few security controls). Assignment of personnel responsibilities and setting up accounts and access control lists to the system and data is another that is a risk factor. In particular, the maintenance phase is where there is high risk. A number of problems can arise where hardware and/or software is replaced or patched. The system at the level of the modules and interacting modules, at a minimum must be re-verified, and the system itself must be re-validated to process data. Often modifying the original system can inadvertently create vulnerabilities or unwanted exposures. Further, documentation must be updated to reflect the change, particularly when it affects operations and operational processes.

Even the process of phasing out or decommissioning systems or software requires a security risk assessment and impact analysis. For example, decommissioning a system on which another system has a dependency (e.g., that other system is expecting data from the decommissioned system) may leave the related system in a vulnerable state (e.g., waiting with an open port for data transaction from the now non-existent decommissioned system). This is a potential for high risk as it provides an avenue for compromise. Performing a risk assessment whenever there is a significant change to the system environment is essential. Again, it is important to recognize that risk management must occur throughout the project life cycle from inception to termination.

Project Life Cycle IT Security Engineering. Risk management requires the cooperation of the entire organization. The 'weakest link' syndrome permeates the environment and the residual effect encompasses and potentially impacts other IT systems and data. Institutional risk abatement activities for the enterprise provide mitigations for the project life cycle and should be accounted for as part of the risk assessment and mitigation analysis process. While the

MANAGING COMPLEXITY AND CHANGE! INCOSE 2004 - 14th Annual International Symposium Proceedings

institutional risk mitigation processes may benefit the life cycle, they must be carefully weighed and balanced against over risks and their potential impact on them. For example, anti-virus (AV) software reduces risk exposure and the impact of malicious content to the institution. However, its use may also have a negative impact on a requirement on availability of a particular COTS application that may not interact well with the AV real-time scanning. The risk mitigation alternatives and relative value in reducing the risk versus cost need to be evaluated as part of the process. Likewise, the institutional firewall has a positive impact in mitigating some risks in attack scenarios by preventing external port exploits. However, the firewall packet inspection may have an impact on a project requiring high throughput availability. As another example, institutional backup services provide a relatively inexpensive means to mitigate the risk of loss of data. However, there may also be a negative impact if the backups are performed at a critical time when other processes require substantial disk reads and writes or CPU cycles.

These factors must be carefully weighed and balanced. Tool support such as that provided by DDP provides the useful capability to semi-automate this process. It also provides the ability to track risk and to update the assessment as the requirements and environment change. Auditing security risk and mitigation processes is significantly aided by using a detailed risk management approach. Management decisions and traceability for those decisions as well as their impact can be made more easily with the risk analysis available to them. Integrating risk mitigations provided by the institution into the project life cycle helps to identify risks that may be already paid for by the projects and need not be duplicated saving costs. Consequently, some of the mitigations, even though more costly when provisioned independently, may actually be less as the costs are shared across the organization and are already factored into the project costs for institutional support. For this additional reason, it is beneficial to implement an institutional risk assessment and mitigation program as described above. Additionally, it is more cost effective when risk mitigation tools and the availability of domain experts are shared institutionally; and as a side benefit, it is likely the tools will be of higher quality and more effective in the environment.

For the institution, having the projects perform risk assessment and mitigation as part of the SDLC, helps the organization to understand the security needs of the organization and provide the capability for full-cost accounting for both the institution and the project. Further, it provides for greater accountability for risk assessment, mitigation, and acceptance in the project and the institution. The organization benefits by approaching IT security risk mitigation from both sides.

Conclusion

Applying a risk management process to IT security is a critical activity to prevent loss or compromise of CIA. This is especially true for organizations that are responsible for HIPPA (Health Insurance Portability And Accountability Act) regulations. An overall architecture to manage IT security risk will enable organizations to understand these risks better, including the likelihood of success, the potential for damage if successful, the effectiveness and cost of mitigations. It will allow managers the ability to make informed decisions on mitigating risk and accepting residual risk, along with the costs associated with them. Such a methodology applied as a systems engineering practice both institutionally and in the SDLC at the project level enables the organization to respond quickly and more effectively to new risks as the environment and technology changes over time. Further, it provides for greater accountability for risk assessment, mitigation, and acceptance both within the project and the SDLC, and institutionally enterprise-wide. The overall approach aids IT security risk management by coordinating the risk

MANAGING COMPLEXITY AND CHANGE!
INCOSE 2004 - 14th Annual International Symposium Proceedings

activities, providing better visibility into the IT security risks, and taking into account the costs to mitigate risks, and the effectiveness of the mitigations identified. While such an approach is not a panacea for eliminating risk, it does provide the capability for managing IT security risk through a formal security engineering process.

Acknowledgement

The research described in this paper was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement by the United States Government or the Jet Propulsion Laboratory, California Institute of Technology.

References

- Akao, Y. 1990 *"Quality Function Deployment"*, Productivity Press, Cambridge, Massachusetts.
- Anderson, R. J., *"Security Engineering: A Guide to Building Dependable Distributed Systems,"* John Wiley & Sons, 2001.
- ArcSight, *"TruThreat Visualization Software"*, 2003, downloaded from the Internet on 10-01-2003, <http://www.arcsight.com/>.
- Bishop, M., *"Computer Security: Art and Science"*, Addison-Wesley Pub Co., 2002.
- Cornford, S.L., Feather, M.S., Dunphy, J.R., Salcedo, J. and Menzies, T., "Optimizing Spacecraft Design – Optimization Engine Development: Progress and Plans", *Proceedings of the 2003 IEEE Aerospace Conference* (Big Sky, Montana, March 2003), pp 8-3681 – 8-3690.
- Feather, M.S., Cornford, S. L., and Moran, K., "Risk-Based Analysis And Decision Making In Multi-Disciplinary Environments," *Proceedings of IMECE'03 2003 ASME International Mechanical Engineering Congress & Exposition* Washington, D.C., November 16–21, 2003.
- Feather, M.S., and Cornford, S. L., "Quantitative Risk-based Requirements Reasoning", *Requirements Engineering (Springer)*, Vol 8 No 4 2003, pp 248-265.
- GAO-03-98, Government Accounting Office (GAO) Audit: *"Major Management Challenges and Program Risks: Department of Defence,"* GAO-03-98, January 2003, downloaded from the Internet on 10-01-2003, <http://www.gao.gov/pas/2003/>.
- Gilb, T., *"Risk Management: A practical toolkit for identifying, analyzing and coping with project risks"*, downloaded from the Internet on 11-11-2003, <http://www.gilb.com/>.
- Howard, M., LeBlanc, D. C., *"Writing Secure Code"*, 2nd Edition, Microsoft Press, 2002.
- McGraw, G., *"Software Risk Management for Security"*, Citigal White Paper, 1999, accessed on the Internet on September, 2003 at <http://www.cigital.com/whitepapers/>.
- NASA CRM Resource Center website, downloaded from the Internet on 11-14-2003, <http://www.crm.nasa.gov/knowledge/default.html>.
- RiskWatch, *"Security Risk Management (SRM) software solutions for government and industry"*, information downloaded from the Internet on 10-10-03, <http://www.riskwatch.com/>.
- SEI, Carnegie Mellon University Software Engineering Institute, *"OCTAVE Method,"* 11-11, 2003, available at <http://www.cert.org/octave/methods.html>.
- Stoneburner G., Goguen, A., and Feringa, A., "Risk Management for Information Technology Systems," The National Institute of Standards and Technology Special Publication 800-30, 2001.

MANAGING COMPLEXITY AND CHANGE!
INCOSE 2004 - 14th Annual International Symposium Proceedings

Witty, R., "Successful Elements of an Information Security Risk Management Program,"
Gartner Symposium ITxpo, U.S. Symposium/ITxpo, Orlando, Florida, 6–11 October, 2002.

Biography

Dr. David P. Gilliam is Principal Investigator for the NASA IV&V Center Initiative, “Reducing Software Security Risk through an Integrated Approach,” an ongoing research project with Matt Bishop of UC Davis. He is involved in Security Research, and the evaluation, design, and implementation of IT security products at JPL. He is also Chair of the IEEE WETICE Enterprise Security workshop. Portions of his research can be viewed at: <http://rssr.jpl.nasa.gov>.

Dr. Martin S. Feather is a Principal in the Software Quality Assurance Group at the Jet Propulsion Laboratory, California Institute of Technology. He works on developing research ideas and maturing them into practice, with current activities in the areas of software validation (analysis, test automation, V&V techniques) and of early phase requirements engineering and risk management. He works on the Defect Detection and Prevention effort (led by Dr. Steve Cornford – see <http://ddptool.jpl.nasa.gov>), and has been the primary architect and developer of DDP’s software. For more details, see <http://eis.jpl.nasa.gov/~mfeather>.